International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

B.ED STUDENTS AWARNESS ON CYBER SECURITY

Dr. Manju Badhwar
Principal
Satpriya College Of Education
Rohtak

ABSTRACT

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber attacks and digital spying are the top threat to national security, eclipsing terrorism. This paper underlines the scope and association of the cyber security education for the B.Ed. Students and their existing awareness.

INTRODUCTION

Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling

ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

physical access to the hardware, as well as protecting against harm that may come via network access, dataand code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

The field is of growing importance due to the increasing reliance of computer systems in most societies. Computer systems now include a very wide variety of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things – and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi and other wireless networks.

A vulnerability is a system susceptibility or flaw, and many vulnerabilities are documented in the Common Vulnerabilities and Exposures (CVE) database and vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. An exploitable vulnerability is one for which at least one working attack or "exploit"exists.

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.
Denial-of-service attack

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

NATIONAL CYBER SECURITY POLICY ON EDUCATION IN INDIA

The government released the first draft of the National Policy on Cyber-security in July 2013. The policy aims at building a secure and resilient cyberspace for citizens, businesses and Government. The full document can be accessed here at: National Cyber Security Policy 2013. As TRAK.IN article says, the policy is very superficial and lacking-in-details, especially for a document which the government has been trying to draft for more than a year now. Given the inherent vagueness of the policy and while awaiting any further clarification from the government, one can presume that the effect of this policy will be felt by organizations in sectors whose relevance to cyber-security would be mildly appreciable. This concern is punctuated by the fact that the policy simply terms all concerns as 'cyber threat' instead of distinguishing clearly between 'national cyber security threat' and 'cyber crimes'. The former needs a much graver concern than the latter. And by failing to appreciate the difference in the policy itself, there is a high potentiality of the government interference in cyber-security concerns of private sector to an extent more than what is required. For the sake of analysis, one can evaluate the overall exposure of a firm to the policy along 3 dimensions, cyber exposure, national security exposure and global exposure. The ultimate measure of impact would be the weighted sum of all these three factors.

Cyber exposure, is the proportion of total operations that happens on the cyber space. National security exposure, measure of how critical the operations of an organization to the national security. Global exposure, measure of the geographical spread of the operations of the firm. Global exposure is especially contentious given the cross-border laws and regulations involved. For example, IT firm working on defense project of a foreign country would score high on all factors whereas an education-services firm providing e-lessons to kids in rural India would score high on the first indicator but low on the other two etc.

The gravest concern in any national policy or any regulation for that matter is the entry barrier it poses to the new entrants. The world today is being increasingly 'cyberized'. An ever increasing

ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

amount of economic activity has shifted to the cyber-space, e-commerce and e-banking, being highly recognized developments. But in a way these developments and the larger proliferation of e-firms in India was facilitated by the lack of strait-jacket regulations in the sector. Such a situation whose credibility could be questioned still served as the jumping board for a large section of self-styled entrepreneurs who couldn't circumvent the regulations choking the conventional entrepreneurial environment in the nation. I wouldn't be surprised if difficulty in procuring affordable real estate at the appropriate time was stated as the primary and availability of credit as secondary of the greatest challenges to healthy entrepreneurial activity in the country. In the last few years, we have seen the rise of numerous multi-retail online stores, e-outlets for major brands, online bazaars for wholesale sell/buy etc. By integrating the operational space and logistical platform into one portal, the firms were able to cut down on a lot of administrative and operation costs. Such a cut-back helped numerous firms to compete at miniscule differences in profit-margins.

The National Optical Fiber Network being built by the Bharat Broadband Network Limited working in coordination with other PSUs, aims to provide pan-India internet connectivity. This is will provide all of the existing 2.5 lakh (approx.) Gram Panchayats with internet connectivity. This opens a whole new dimension to the rural economic sphere. Financial inclusion, Spot futures for farmers, e-medicine etc. are just some of the many boons to follow. But over and above the rest, it is education and medicine whose exposure to internet in rural India, I value the most, given their potential impact on the overall development of the nation.
In the post-liberalization era, given the demographic dividend of the nation, education has been a great attraction for both the profit and non-profit sector. In the for-profit sector, the attraction is by virtue of the potential market size in all the sections of primary, secondary and higher education sector. In the non-profit sector, entrenched poverty, large-scale illiteracy etc. brought the world's attention to the development needs of the nation. Education was seen as a solution to all the problems with the presumption that it will lead to increased employability. The boom of the IT sector indeed made this wish true till the end of the first decade of the millennium. But as

job prospects fall in tandem with the employability of India's educated youth, the focus on education has intensified like never before. There are hundreds of NGOs and tens of Foundations working in the country towards making education more accessible to the poor as well addressing issues like gender discrimination, social inclusion of physically/mentally challenged children and class based discrimination. But given, the amount of money and effort that has gone into the sector, most of the veterans in the field agree that the expected impact hasn't been yet achieved. The inefficacy of philanthropic interventions has brought about a certain pessimism in the minds of development sector professionals. But the gloom is parallel witnessing the rise of technology based education solutions for children in India. Educom, Pearson, Pratham etc. are just some of the organizations that are in this e(du)-sphere.

Many of these organizations and many other start-ups in the pipeline are greatly relying on this optical fiber network to scale-up their ventures and reach the remote areas where access to quality education has always been marred by lack of competent teachers and other supportive resources. These firms in the process of scaling up will inevitably fall under the purview of the National Cyber Security Policy given the wide mandate the policy has provided for itself. Also due to lack of distinction between critical levels of cyber-activities with respect to national security, for the purpose of compliance with the policy, the policy stands in the position of possibly imposing a higher entry cost for firms and organizations. Even with conservative estimates, the education market in India is worth tens of billions in US dollars. The demography to be served is also widely distributed providing a fertile ground for a new wave of entrepreneurs in the sector. This is a great opportunity for Indian youth to build upon the IT expertise we have developed, thanks to the IT revolution in the country. As things stand, there is a great demand and great possibility for quality supply especially given that the beneficiaries are going to be lower sections of the economic hierarchy in the country, we should be all the more supportive of the momentum. In the light of the above, the fear is that, the Cyber Security Policy could be interpreted much widely than essential for securing national security. This will be a great obstacle to the blossoming online entrepreneurs/development professionals in delivering the

targeted products/interventions to the target population. As of now, there is no idea about the compliance cost for this policy. But one can envisage the difficulties that might arise given the bureaucratic history of the Indian state.

The National Cyber Security Policy 2013, is a step in the right direction but its inherent vagueness combined with the discretionary powers of the State bureaucrats could quell the upcoming online entrepreneurs by increasing their entry cost. This is especially bad for the education sector given the rising number of tech-based solutions for mitigating the education problems of the nation. We will have to be vigilant about the evolution of this policy into a full-fledged bill and strive to correct any deviation of this policy into areas where it could be a bane rather than a boon.

With an estimated need of over five lakh cyber security professionals in the coming few years, India woefully lacks the plans to meet the target. All it has now is just 22,000 identified trained security experts while the IT and ITES sector is growing at a decent pace.

About 42 million Indians are exposed to cyber threats and an estimated loss of 8 billion US $ is projected but the government doesn't have the apparatus to tackle the issue nor any concrete plans to create the necessary workforce.

"No university or college offers a course covering the whole gamut of cyber security," says Jay Bavisi, president of EC-Council, a global certification and training organisation in information security. Though the University Grants Commission (UGC) has asked the universities and colleges to prepare and offer a course in cyber security there is hardly any idea among the varsities on how to go about it. "The UGC direction is not clear on what information security is all about," Mr. Bavisi says.

CASE (SCENARIO)

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

CHI-SQUARE TEST

(CYBER SECURITY EDUCATION PRACTICES, GENDER)

Follows Practices	Gender	(In Years)	Frequency
N		M	20.00
N		M	30.00
N		F	10.00
N		F	13.00
N		F	15.00
N		M	9.00

DESCRIPTION OF THE NULL AND ALTERNATE HYPOTHESIS

H_0 (Null Hypothesis): The CYBER SECURITY EDUCATION Practices are followed and there is no key impact on the school"

H_0 (Alternate Hypothesis): The CYBER SECURITY EDUCATION Practices are not followed and there is major or key impact on the school"

To analyze the results of the null as well as alternate hypothesis, the following statistical analysis has been performed.

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Experience	100	2.6907	.46460	2.00	3.00

Chi-Square Test

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

Experience			
	Observed N	Expected N	Residual
1-2Y	33	48.5	-18.5
2-3Y	67	48.5	18.5
Total	100		

Test Statistics

	Experience
Chi-Square	14.113[a]
Df	1
Asymp. Sig.	.000

a. 0 cells (0.0%) have expected frequencies less than 5. The minimum expected cell frequency is 48.5.

INTERPRETATION AND EXPLANATION

The Hypothesis that "The CYBER SECURITY EDUCATION Practices are followed and there is no key impact on the school" is hereby REJECTED because :

From the Chi-Square Analysis, for the degree of freedom 1, the value of Chi-Square (χ^2) is 14.113. Additionally, it indicates that the Significance Value (0.000) is less than the Threshold Value of 0.05 (or within the range or 0.05). This suggests that the Hypothesis is Rejected and it is evidently found that the schools are not following the CYBER SECURITY EDUCATION practices for upliftment and benefits of the education system.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

It is very apparent from the analysis of the frequency that there is quite difference between the observed and expected count. The residual found is giving difference a lot which means that the experience level and the negation count is related regardless of the gender and other parameters.

CASE (SCENARIO)

ONE WAY ANOVA (ANALYSIS OF VARIANCE)

IMPACT OF 360 DEGREE FEEDBACK FOR TEACHERS AND GENDER

DESCRIPTION OF THE NULL AND ALTERNATE HYPOTHESIS

H_0 (Null Hypothesis): "There is no effect of any CYBER SECURITY EDUCATION Policy (360Degree Feedback) in the School"

H_0 (Alternate Hypothesis): "There is major effect of the CYBER SECURITY EDUCATION Policy (360Degree Feedback) in the School for retaining the talented staff and the manpower"

To analyze the results of the null as well as alternate hypothesis, the following statistical analysis has been performed.

Descriptives

Gender

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
StronglyAgree	16	1.3750	.50000	.12500	1.1086	1.6414	1.00	2.00
StronglyDisagree	4	2.0000	.00000	.00000	2.0000	2.0000	2.00	2.00
Total	20	1.5000	.51299	.11471	1.2599	1.7401	1.00	2.00

Test of Homogeneity of Variances

Gender

Levene Statistic	df1	df2	Sig.
54.000	1	18	.000

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M57-072014

ANOVA

Gender

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.250	1	1.250	6.000	.025
Within Groups	3.750	18	.208		
Total	5.000	19			

INTERPRETATION AND EXPLANATION

The Null Hypothesis that "There is no effect of any CYBER SECURITY EDUCATION Policy (360Degree Feedback) in the School" is hereby REJECTED because :

The Significance Level of 0.25 is less than the threshold value of 0.05 indicating that the null hypothesis can be REJECTED. In conclusion, it is apparent that there will be huge effect of integrating the new policy for the system so that the overall scenario can be enhanced.